

Anleitung zur Einrichtung und Nutzung einer 2-fach Authentifizierung (Token) - Teil II: Benutzer



Diese Anleitung wurde mit Untis / WebUntis 2018 erstellt. Als Untis- Express-Anwender oder bei Untis Multiuser gehen Sie bitte analog vor.

Die Anleitung ist zur Einführung einer 2-fach-Authentifizierung (auch Zwei-Faktor-Authentifizierung oder 2FA genannt) an Ihrer Schule gedacht. Sie dient dem Identitätsnachweis eines Nutzers mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren): das bisherige Passwort + eine Nummer, die durch einen sog. Token generiert wird. Die Anleitung bezieht sich auf einen Token der Firma Token2.com. Die Tokens dieses Herstellers wurden mit WebUntis positiv getestet. Tokens anderer Hersteller wurden bisher nicht getestet und sind daher nicht zwingend kompatibel zu WebUntis.

- 1) Der Token kommt mit der Post → auf der Rückseite befindet sich eine 10-stellige Nummer (Zeichenfolge) + Strichcode. Hierbei handelt es sich um die Seriennummer, nicht um das sog. „shared secret“.
- 2) Es kommt eine E-Mail vom Hersteller / Händler, die a) die 10-stellige Nummer enthält + b) eine lange Zeichenfolge (> 20 Zeichen). Diese lange Zeichenfolge wird in WebUntis im Feld „Schlüssel“ eingegeben. Hierbei handelt es sich um das „shared secret“.

Im Wesentlichen gibt es 2 Anlässe, weswegen Sie die 2-fach-Authentifizierung nutzen möchten: Sie handeln auf Anweisung der Schulleitung oder Sie möchten einfach selbst den Zugang zu Ihrem Account sicherer machen.

- a) Eigenverantwortliches Einrichten der 2-Faktor-Authentifizierung:

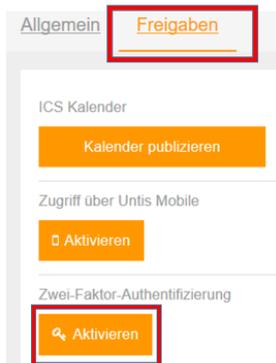
Wenn Sie sich als Benutzer eingeloggt haben, klicken Sie bitte auf die Taste links neben dem Abmelden: auf „Profil“.



Anleitung zur Einrichtung und Nutzung einer 2-fach Authentifizierung (Token) - Teil II: Benutzer



Unter Freigaben aktivieren Sie dann die Zwei-Faktor-Authentifizierung:



Fahren Sie fort bei Punkt c)

b) Die Schulleitung schreibt die 2-Faktor-Authentifizierung vor

Ihr WebUntis-Administrator (im Auftrag der Schulleitung) hat eine 2-fach-Authentifizierung an Ihrer Schule eingeführt. Sie als Benutzer sind nun angehalten, dies für Ihr Benutzer-Konto einzurichten. Darüber werden Sie unmittelbar nach Ihrem Login informiert:

Zwei-Faktor-Authentifizierung - Aktivierung (1/2)

Sie müssen die Zwei-Faktor-Authentifizierung einrichten.

Mit Google Authenticator können Sie Ihren Benutzerzugang zusätzlich schützen.

Authenticator ist ein kleines Programm, das Sie auf Ihrem Smartphone installieren können. Es erzeugt einen Code, der beim Anmelden zusätzlich zum Passwort abgefragt wird.

Sie benötigen dafür ein von Google Authenticator unterstütztes Smartphone.

Zurück Weiter

Anleitung zur Einrichtung und Nutzung einer 2-fach Authentifizierung (Token) - Teil II: Benutzer



c) die Aktivierung

Klicken Sie bitte die untere Variante an und gehen auf „Aktivieren“.

Zwei-Faktor-Authentifizierung - Aktivierung (2/2)

Mit der Zwei-Faktor-Authentifizierung können Sie Ihren Benutzerzugang zusätzlich schützen.

Eine Authenticator App am Smartphone oder ein Security-Token erzeugt einen Code, der beim Anmelden zusätzlich zum Passwort abgefragt wird.

Bitte wählen Sie

- App Authenticator (z.B. FreeOTP oder Google Authenticator)
- Security-Token (Hardware mit einem One-Time Password-(OTP-)Generator)

Zurück

Aktivieren

Danach geben Sie bitte die **lange Zeichenfolge (> 20 Zeichen)** ein, die Sie mit der E-Mail des Händlers bekommen haben.

Zwei-Faktor-Authentifizierung - Aktivierung (2/3)

Sie benötigen ein Security-Token.

Bitte geben Sie den Schlüssel ein, den Sie zu Ihrem Security-Token bekommen haben. Wählen Sie bitte wenn notwendig die richtige Codierung (Base32 oder Hex) des Schlüssels.

Schlüssel

- BASE32
- HEX

Zurück

Weiter

Anleitung zur Einrichtung und Nutzung einer 2-fach Authentifizierung (Token) - Teil II: Benutzer



Nun werden Sie aufgefordert, die erste Zahl mit dem Token zu generieren. Diese Zahl erhalten Sie, indem Sie auf die Taste neben dem Anzeigefeld drücken.



Zwei-Faktor-Authentifizierung - Aktivierung (3/3)

Bitte geben Sie den aktuellen Bestätigungscode ein, den Ihr Security-Token anzeigt.

Zurück

Aktivieren

Anschließend klicken Sie auf „Aktivieren“.

Anleitung zur Einrichtung und Nutzung einer 2-fach Authentifizierung (Token) - Teil II: Benutzer



Ab jetzt funktioniert jedes Einloggen folgendermaßen:

- 1) Sie geben wie gewohnt Ihr erstes Passwort ein

A screenshot of the WebUntis login interface. At the top, there is a dark grey header with a white "Login" button and the "WebUntis" logo. Below the header, the word "Login" is displayed in orange. There are three input fields: the first contains "untis bw", the second contains "Ander", and the third is empty with a blue eye icon. Below the input fields are two buttons: an orange "Login" button and a grey "Abbrechen" button. At the bottom, there is a link that says "Passwort vergessen ?".

- 2) Im zweiten Schritt geben Sie die Nummer ein, die der Token neu generiert.

A screenshot of the WebUntis login interface during the second step of authentication. The header is the same as in the previous screenshot. Below the header, the text "Google Authenticator" is displayed in orange. Below that, the instruction "Bitte geben Sie Ihren Bestätigungscode ein." is shown. There is an input field containing six hash symbols "#####" and a red "x" icon to its right. Below the input field, a red error message reads "Die Eingabe muss genau 6 Zeichen lang sein". At the bottom, there are two buttons: an orange "Login" button and a grey "Abbrechen" button.